

● 論 説 ●

ドイツ信頼役務法の検討

法科大学院教授 米丸 恒治

- I はじめに
- II 信頼役務法制定の経緯と背景
- III 信頼役務法の概要
- IV 若干の検討
- V おわりに

I はじめに

本稿は、別稿¹で課題として残しておいたドイツの信頼役務法（Vertrauensdienstegesetz v. 18. Juli 2017, BGBl. I S. 2745）の制定経緯とその概要を紹介し、ドイツにおけるeIDAS規則の執行のための法制度を検討しようとするものである。同法は、ドイツがeIDAS規則を執行するために制定した「指令1999/93/ECの廃止ならびに域内市場における電子取引のための電子識別および信頼役務に関する2014年7月23日欧州議会および理事会規則（EU）第910/2014号の施行のための法律（eIDAS施行法）」（法律2017年7月18日）²の第1条で制定されている法律である。前稿で検討したように、eIDAS規則は、EUの域内で直接適用される規則の形式で制定されており、従来の電子署名指令のように各国の国内措置を基本的には必要としていない。しかし、監

1 米丸恒治「eIDAS規則－EUにおける新署名認証基盤法制－」専修ロージャーナル14号（2018年）27頁。eIDAS規則の邦訳としては、さしあたり、米丸恒治訳「「指令1999/93/ECの廃止ならびに域内市場における電子取引のための電子識別および信頼役務に関する2014年7月23日欧州議会および理事会規則第910/2014号（2014年8月28日EU官報L257/73頁）（松本恒雄・多賀谷一照編集代表『情報ネットワークの法律実務』）7359-7386頁（加除式，2015年）参照。

2 Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz) v. 18. Juli 2017, BGBl. I S. 2745. 法案と提案理由は、BT-Drucks. 18/12494 v. 24. 5. 2017参照。信頼役務法の試訳は、本号239頁以下参照。

督機関の指定や罰則規定の制定などのように、eIDAS規則を施行するための国内法は必要であり、ドイツの信頼役務法も必須の制定事項としては、監督機関や罰則の制定にとどまってもよい法律であった。しかしながら現実に制定された信頼役務法は、それにとどまらない規定を盛り込んでおり、信頼役務の長期的な安全性に関わる規定をも盛り込む注目すべき法律であることから、本稿でその概要を紹介し、若干の検討を加える事とした次第である。同法の実施のための委任命令（「信頼役務令（Verordnung zu Vertrauensdiensten（Vertrauensdiensteverordnung – VDV）³⁾」）も含め、以下では検討の対象としたい。

II 信頼役務法制定の経緯と背景

eIDAS規則が制定される以前は、EUの電子署名指令⁴⁾が国内措置を求めて制定され、ドイツでは、その国内措置として、当初のデジタル署名法⁵⁾を改正する新電子署名大綱法⁶⁾が制定施行されてきたのであった。

その後、eIDAS規則が制定され、2016年7月1日から、加盟国で直接適用される。

eIDAS規則は、前稿で検討したように、電子署名のみならず、大きな分量をeIDの相互承認に割くと同時に、電子署名以外の電子印（法人の電子署名）、タイムスタンプ（電子日時証明）、電子書留メール、適格電子署名検証、適格電子文書保存役務のこれら新たな「信頼役務（トラストサービス、Vertrauensdienste）」を規制対象とし、一定の法的推定効を与える「適格電子署名」等の適格役務の要件を抽象的概略的に定める規則である。eIDAS規則は、その規制対象を新たな信頼役務へと広げた一方で、eIDAS規則のみでは、従来の電子署名法および電子署名令が実施し

3 Verordnung zu Vertrauensdiensten (Vertrauensdiensteverordnung – VDV) v. 15. 2. 2019, BGBl. I S.114.

4 その概要と邦訳として、米丸恒治（解説と邦訳）「EU電子署名指令」立命1999年6号276頁参照。

5 デジタル署名法については、その邦訳とともに米丸恒治「ドイツ流サイバースペース規制」立命1997年5号141頁以下（デジタル署名法の邦訳は、いわゆるマルチメディア法の第3条として制定されたものであるが、同186頁以下に掲げている。電子署名に限定しては、米丸恒治「ドイツ・デジタル署名法と電子認証－サイバースペースの不確定性克服の制度基盤の検討－」（立命1997年6号256号31頁（1998年）以下）参照。また、電子署名令は、Verordnung zur elektronischen Signatur (Signaturverordnung - SigV), v. 16. 11. 2001, BGBl. I S. 3074である。

6 デジタル署名法を改正し、EU電子署名指令の国内措置として制定された新電子署名法については、米丸恒治訳「ドイツ新電子署名法」立命2001年5号（2002年）163頁参照。旧法との違いは、旧法が免許制をとっていたのに対し、新法は事前規制がEU指令により制限されたため、認証事業者に対して任意認定制度を取った点である。

てきた電子署名の安全で長期的な利用のための諸規定を十分に置き換えるような、条文の量と質に達していないものとドイツ側では考えられていた。⁷従来、電子署名法制に深く関わってきたロスナゲルの立場からすれば、当初は、当時の旧電子署名法および電子署名令を基本的には存続させることにしてeIDAS規則と重複して、しかも矛盾する規定については、効力のないものとして改正を行うべきである旨、述べていた。⁸規定が抽象的であり、規定の分量としても、例えば旧電子署名法が電子署名のみについて、全25条、署名令が全19条別表2表であるのに対して、eIDAS規則は、信頼役務を含めても電子署名については、13条から34条までの22箇条しか規定をおいていない。しかしその後、連邦経済省は、電子署名大綱法および旧電子署名令を廃止して、eIDAS規則を補完する「信頼役務法」および信頼役務令を制定する立法手続に入ったものである。

連邦政府の参事官草案は、2016年10月18日に策定され、関係団体との協議を経て、2017年3月31日に連邦政府は同法案を連邦参議院に提出し、連邦参議院は、2017年5月2日に3点ほどの小規模な修正をして、同法案が連邦議会に提出された。連邦議会でも、同法案に対しては19条の過料規定の修正、8条のデータ保護規定をEUのデータ保護基本規則（Datenschutz-Grundverordnung）に適合させる修正がなされたほかは、連邦政府提出法案がほとんどそのまま、連邦議会を通過して、2017年7月18日の法律として、連邦官報の同年7月28日版にて公布されたものである。同法の施行により、その第1条として制定された信頼役務法が制定されたのであり、eIDAS規則施行法は2017年7月18日に施行され、それとともに、同法で定められた信頼役務法が2017年7月29日に施行、同時に署名法および署名令は、廃止されることになったのである。

Ⅲ 信頼役務法の概要

信頼役務法は、5章からなっているが、第1章は総則、第2章は、適格信頼役務についての総則、第3章は、適格電子署名および適格電子印について定め、さらに第4章は適格電子書留の送達に関する規定をおき、最後に補則をおいている。

7 たとえば、ロスナゲルは、eIDAS規則は、加盟国の補完的な立法作業がなければ、「抽象的すぎて、不完全でかつ複雑性に劣る」ものであると述べている。Roßnagel, Das Vertrauensdienstegesetz, MMR 2018, S. 31 ff., S. 35.

8 署名法および署名令とeIDAS規則の規定とを比較対照した作業として、Alexander Roßnagel, Das Recht der Vertrauensdienste – Die eIDAS-Verordnung in der deutschen Rechtsverordnung, 2016, S. 43 ff.がある。

1 第1章 総則部分

第1章の総則部分では、本法の適用範囲と所管行政庁、監督権限、責任、データ保護と障害者対応（バリアフリー；Barrierefreiheit）の規定をおいている。

(1) 監督機関の監督の及ぶ範囲については、eIDAS規則のそれに適合しているが、非適格信頼役務事業者にも及ぶ範囲を定めている。これは、日本法の監督権限が、任意の認定を受けた業務についてのみ監督権限を及ぼしていることと際だった監督権限の範囲の差を見せているものである。非適格信頼役務事業者の場合も、様々な不当、不正な業務遂行のために多様な紛争を引き起こす可能性が高いことを考えれば、そこまで範囲を広げているEUの監督機関の権限についての考えは、極めて適切なものと考えられる。

(2) 第2条では、監督機関として、電子署名、電子印、タイムスタンプ、電子書留メールの送達に関連しては、連邦ネットワーク庁（Bundesnetzagentur（BNetzA））⁹が、ウェブ認証に関しては、連邦情報セキュリティ庁（Bundesamt für Sicherheit in der Informationstechnik; BSI）が、監督機関として指定されている。連邦情報セキュリティ庁は、従来から担当してきた技術標準の作成・評価や、暗号アルゴリズムと関連パラメータの評価（電子署名等の安全性に関わる）、技術規格の評価等については、継続して担当するものとされる。

(3) 第3条は、ワンストップ行政手続を認める規定である。

(4) もちろん、監督権限には、営業禁止命令を含む強力な権限が定められていることにも、当然のこととはいえ留意しておく必要がある。監督権限を実効化するために、監督機関に対しては、営業所への立ち入り権限や帳簿の閲覧権限等の諸権限が与えられ、事業者にはそれに対応する協力義務が定められている（第4条、第5条）。

(5) 第6条の責任規定では、事業者のみならず、それが任務を委任した第三者に対しても過失責任を負わせる旨が定められている。

(6) 第7条では、「可能な限り」という限定付きながら、信頼役務事業者に対して、障害者が利用可能な役務の提供を求めている。そして障害者に対して、それら利用可能な役務の情報を提供することも求めているところが注目される。

(7) 第8条は、個人情報保護に関する規定であり、それぞれの事業者がその信頼役務の審査および効力確認を含む役務提供に必要な限りで、第三者の個人関連デー

9 正式名称は、Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnenである。

タの処理をすることができるとする（第1項）。その上で、さらに犯罪または秩序維持犯の訴追、公共の安全または秩序の維持のため、および憲法保護機関等が法的任務を遂行するために送信を求める限りにおいて、個人情報とこれらの管轄機関に送信することが必要であるとしている。裁判所が係属中の手続において転送を求める場合においても、転送は必要であるとしている。また、個人関連データの転送をした場合は、事業者は、その旨を記録にとどめなければならない、当該文書は、12ヶ月間保管することが義務づけられている。これは、一般的なデータ保護法制¹⁰上の義務に存在しない特則である。

2 第2章 適格信頼役務事業者総則

第2章では、適格信頼役務事業者に関する総則的な規定を定めている。

内容的には、トラストリスト、損害賠償への供え、本人確認、証明書の属性、教示規定、証明書の失効手続、長期的な証拠性の保持、業務終了計画、長期的に検証可能な信頼役務についての規定をおいている。

(1) 第9条は、トラストリスト (trusted list; Vertrauenslist)¹¹の発行・管理権限を連邦ネットワーク庁に付与する規定である。

(2) 第10条は、eIDAS規則では具体的に定められていなかった損害賠償への備えの金額を、当該責任を生じさせる事象に起因する損害発生（事故）につきそれぞれ25万ユーロと定めている。具体的には、損害賠償保険の付保や、債務免除保証契約で、法的には対応することを信頼役務令2条で具体的に定めている。わが国の署名法では、手当がされていない損害賠償につき、注目される規定である。

(3) 第11条は、信頼役務における本人確認の手法について、具体的な革新的手法について、連邦情報セキュリティ庁と合意の上で、最小要件を公報で決定することとした（同条1項）。その上で、4年の間隔で定期的に見直すか、または識別手法

10 一般的な個人情報保護法制として、EU全域に直接適用されるいわゆる一般データ保護規則 (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88); GDPRが施行され、わが国でもそれへの対応に注目が集まっている。

11 ドイツのトラストリストは、ドイツのルートCA関係のサイト< <https://www.nrca-ds.de/st/TSL-XML.xml> >(visited on 7.21.2019) で公表されているが、EU全体のブラウザ< <https://webgate.ec.europa.eu/tl-browser/#/> >(visited on 7.21.2019) で適格事業者のリストが閲覧可能となっている。

が十分に安全ではないという合理的な仮定があったり、BSIからの見直しの要請があった場合には見直しを行うこととしている。公報で公示されていない革新的な識別方法は、最長2年まで暫定的に認可されることがありその間にリスクを補うための補足的方法が認められる場合には、当該識別方法が使用されることになる。

(4) 適格証明書 (qualifizierte Zertifikat) の属性 (Attribut) について定めるのが12条である。そこでは、第三者に対する代理権の情報、申請者の職業関連の資格、およびその他の個人関連情報が、属性として適格証明書の中に書き込まれることができる。同条2項では、氏名の代わりに仮名を適格証明書に入力する場合、第三者または各権限機関がその仮名を使用する同意を与えた場合に限り、個人情報の利用が認められている。こうした事項については、電子印の場合にも準用される。電子印の属性として法人の代表関係を示すときには、法人により代表関係が証明される必要がある(3項)。

(5) 旧電子署名法は、セキュリティ対策上および法的に重要な事項については、クライアントに教示しなければならない義務を事業者に課していたが、新法では、13条において、「一 提供される信頼できる役務の安全性とそれらの信頼できる使用に貢献するために必要な措置に関する情報を提供し、適切な情報機会、特に適格な信頼役務のために製品の製造業者によって提供される情報と監督機関によって提供される情報役務に注意を向ける。／二 既存の署名、電子印、またはタイムスタンプのセキュリティ価値が時間の経過によって減少する前に、必要に応じて第15条の適格な電子署名、電子印、またはタイムスタンプ付きのデータを適切な手段で新たに保護すること。／三 提供された適格信頼役務の法的効果について教示するため。」の3点を教示すべきものとして継続させている。暗号技術を使った電子署名ならではの重要事項として、安全性と、暗号の危殆化、適格信頼役務の法的効果を周知させて利用者保護的な目的を達成しようとしているものである。これらは、重要な教示事項である。特に、第2号の安全性低下で対応する措置についての教示義務は、信頼役務が暗号技術の安全性(暗号が破られないこと、解読されないこと)の一定のレベルに依拠していることによる技術的制約事項として重要な情報であることに注目しておきたい。

(6) 法14条は、適格証明書の失効についての規定である。法は、「一 適格証明書を発行された者がそれを要求するとき /二 適格証明書が、規則(EU) 2014年910号の附属書I、ⅢおよびⅣの虚偽の情報に基づいて発行されているとき /三 当該事業者が自分の活動を中止し、他の適格信頼役務事業者によって継続されてい

ないとき／四 事実が以下の仮定を正当化するとき／a) 適格証明書が偽造されているか、または十分に偽造防止されていないこと。／b) 使用されている認定電子署名作成装置または認定電子印作成装置にセキュリティ上の欠陥があること。」を法定失効事由として定めており、さらに契約によりその他の失効事由をも定めることができるとする。証明書に記載された属性が変更された場合も、「一 代理権がなくなるか、または／二 適格証明書に記載された後の、公的および専門的またはその他の個人データの前提条件が喪失したとき」には、証明書の失効の要求を受けて失効させる手続を定めている。

(7) 長期の証拠保持の必要性がある場合には、15条において適格電子署名され、適格電子印が押され、または適格タイムスタンプが付されたデータは、時間の経過の結果として既存の署名、電子印またはタイムスタンプのセキュリティ価値が低下する前に適切な手段によって新たに保護されなければならない、新しいセキュリティ確保は、最先端技術に従ってこれを行う必要があるとの規定において対応している。電子証拠の長期的な利用を考慮すれば、必要な措置についての規定であり、条文上も明確化している点を筆者は従来から注目してきた。旧法では、署名令 (SigV) 19条で定められていた事項を、法律レベルに格上げしたものである。

(8) また、わが国の電子署名法に欠けている点として、事業の休廃止時の措置の問題がある。eIDAS規則上は、終了計画を立てさせることを適格信頼役務事業者の義務としているのみであり (eIDAS規則24条2項 (i))、具体的な休廃止時の措置については、規定がない。信頼役務法では、16条で、活動の終了、適格資格の撤回または破産手続の開始を求めるために必要なすべての措置を終了計画において提供しなければならないとし、その上で、事業者の活動は中止され、電子署名および電子印等に関連して発行されたすべての適格証明書失効情報も含めてすべてを他の適格信頼役務事業者を引き継ぐか、同条5項で定められている連邦ネットワーク庁によって形成されたトラスト基盤へと引き継ぐこととされている。他の事業者に引き継ぐことができない場合には、連邦ネットワーク庁が最終的な引受先となって、結果的に長期的な検証可能性を確保しようとしているのがドイツの旧署名法時代からの法的仕組みであり、この点が電子署名を長期間証拠として利用しようとする観点から注目される点である。同様の考え方で法整備¹²をしている国としてオーストリアがあることも紹介しておきたい。

12 オーストリアでは、「署名役務および信頼役務法 (Signatur- und Vertrauensdienstegesetz v. 8.

3 署名および電子印について

第3章では、署名および電子印についての特別規定をおいている。

電子署名および電子印については、eIDAS規則が比較的詳細な規定をおいているため、信託役務法では特別法としては、適格電子署名生成装置についての認定機関についての規定を置くにとどまっている。法17条は、規則25条から40条までの規定に対する補則規定として指定機関の規定をおいており、認定機関法 (AkkStelleG¹³) 1条1項により認定機関が民間機関として必要な要件を満たしているときは申請により、必要な認定機関の要件を満たすものとして扱うこととしている。

4 電子書留の送達

第4章は、電子書留の送達について一箇条の規定を置く。

法18条は、電子書留送達役務について規定しているが、その内容は、信託役務としての適格送達役務の要件を、De-Mail¹⁴法18条3項の認定要件の範囲に限定すべきであることを示している。すなわち同項が定めている認定要件として、De-Mail役務に必要な専門性・信頼性、適切な損害賠償の備え（1事故あたり25万ユーロ）、業務の信頼性・安全性に係る技術的および組織的要件、業務の構成および運営に関してデータ保護上の要件の4点にかかる審査基準を証明するための細目を具体化していることになる。

Juli 2016, BGBl.(Österreich) I Nr. 50)」を定めて、事業者の業務休廃止等に際しての引き継ぎ義務を定めるとともに、その義務が果たされないときは、ドイツとはほぼ同様であるが、監督機関がその信頼基盤にて事業者の費用で証明書データベースをさらに運用するものとするとして定めている（第9条第2項）点は注目される。なお、オーストリアでは、ドイツ法では以前定めていた（今回の信託役務法への改正により、証明書失効後30年検証可能性を維持するとの条項は欠落している。）30年もの長期にわたる事業者の文書保存義務を現行法でも維持している（10条3項）ことを付言しておきたい。

13 Gesetz über die Akkreditierungsstelle v. 31.7.2009, BGBl. I S. 2625. 同法1条1項では、認定は、高権的な任務であり、国内の認定機関によりなされる権限がある旨が定められている。

14 De-Mailとは、ドイツで信託役務法に先立ち立法されていた本人確認認証付きの電子書留配信サービスである。De-Mailについては、さしあたり米丸恒治「ドイツDe-Mailサービス法－安全で信頼性ある次世代通信基盤法制としての認証付メール私書箱法制－」多賀谷一照・松本恒雄編『情報ネットワークの法律実務』第一法規、（加除式、2011年）2731頁以下、同「ドイツDe-mailサービス法の成立－安全で信頼性ある次世代通信基盤法制としてのドイツ版電子私書箱法制－」行政&情報システム2011年6月号30頁以下参照。また、同法の和訳としては、渡辺富久子「訳」「Deメール法」外国の立法261号（2014年）64-78頁がある。

5 過料および委任立法

第5章は過料規定と委任立法の根拠規定をおいている。

罰則について定める法19条は、その1項で、信頼役務法に違反する4つの罰則（過料）規定をおいており、第2項では、eIDAS規則に違反する9つの罰則規定をおいている。わが国の電子署名法と比較すると、罰則規定が多いように思われるが、ロスナゲルによれば、普通で最高2万ユーロ、eIDAS規則違反の4つの規定では最高10万ユーロという罰則は、「著しく低い」ものとの評価がなされている。¹⁵

法20条では、旧署名法と同様に、信頼役務の利用可能性および利用に関するより詳細な要件を定める委任立法を定めることを連邦政府に委任している。すでに、定められ施行されている信頼役務令¹⁶は、1条でバリアフリーの要件、2条で適格信頼役務事業者の損害賠償への備えの細目規定、3条で信頼役務のための適格証明書の発行の記録、4条で適格証明書の継続的な検証可能性についての備え、5条で命令910/2014号（eIDAS規則）の付属書IIによる署名生成装置についての届出、の各規定をおいている。

以上が、eIDAS規則施行法の第1条で制定された信頼役務法の概要である。

6 eIDAS規則施行法のその他の規定

eIDAS規則施行法は、全部で8つの法律を改正し結果的に、11条において結果的な改正として46の法令が改正されている。ほとんどの改正部分が、署名法を参照していた条文をeIDAS規則の適当な条文への参照へと置き換える規定となっている。適格電子署名について定めてきた文言については、eIDAS規則でも変わっていないので、特に変更はなされていない。

7 信頼役務の証拠力についての規定

eIDAS規則施行法は、証拠規定の適合のためには、その10条3項で、民事訴訟法371a条第1項第2段の署名法をeIDAS規則に文言上変更する規定を含んでいるのみであり、電子文書の証拠力についての規定そのものには変更を加えていない。署名法という根拠法令をeIDAS規則に変更したのみである。

15 Roßnagel, a.a.O. (N.7), S. 35.

16 前掲・注3参照。

IV 若干の検討

以上が、信託役務法の概要である。以下では、本稿の問題関心から重要と考えられる事項を取り上げ、若干の考察を加えることとしたい。

1 監督機関とその監督範囲

信託役務がその信頼性を保つように、信託役務事業者に対する監督が適正になされることは必須の条件といえる。従来の電子署名法においても、ドイツの署名法においては、適格電子署名の証明書を発行する認証事業者に対しては、任意の認定制度を設けて認定を受けた認証機関に対する監督権限を行使することとしていたほか、認定を受けない適格証明書を発行する認証機関に対しても届出義務を課して、その設備や人員、活動状況等に適格要件を満たさない問題がある場合は、事後的な監督権を行使して調査および措置命令をなす権限を定めていた。¹⁷

行政法の常識として、監督権限を適正に及ぼすためには、そのための法律の根拠が必要であり、監督権限の法定が求められるところ、わが国の電子署名法では、認定認証業務以外の認証業務を行う事業者への監督権限が法定されておらず、そのために、せいぜい法律に根拠を有しない行政指導ができるのみの状況になっている。これでは、認証業務に問題がある事業者の活動をめぐって必要な監督ができないという重大な問題点がある。eIDAS規則および信託役務法4条にあっては、適切な監督権限の行使ができるように、根拠規定を法定していることが、当然のこととはいえ、注目されなければならない。

その点に関して、eIDAS規則では、その17条で、監督機関についての定めを置き、加盟国にしかるべき監督機関を指定させるとともに（同条1項）、監督機関は、「監督機関の役割は、次の各号とする。／（a）適格信託役務事業者及び適格信託役務事業者が提供する適格信託役務が本規則で定められた要求事項に適合していることを保証するために、事前及び事後の監督活動を通じて指定する加盟国の領域に設立された適格信託役務事業者を監督すること／（b）非適格信託役務事業者又はそれらが提供する信託役務が本規則で定められた要求事項に適合しないと推測される場合は、必要に応じて、指定加盟国の領域に設立された非適格信託役務事業者に関し

17 旧署名法19条および20条。拙訳・前掲注6）175頁。拙稿・前掲注1）44頁参照。

て、事後的監督活動を通じて措置を講じること」(同3項)として、信託役務に関わる必要な範囲での監督権限を有するように措置されている。これによって、信託役務法4条とあいまって、信託役務に関する問題が生じたときも立ち入り検査や措置命令などの事後的な監督手段が行使される法的根拠が与えられていることになり、究極的にはユーザ及び署名依拠当事者にとっても必要な監督を予定した信託しうる信託役務市場が確立することになる。

2 信託役務事業者の責任と損害賠償への備え

信託役務をめぐる損害賠償についても、EUのeIDAS規則には注目すべき点がある。

eIDAS規則は、その13条で、損害賠償責任とその立証責任についての規定をおいている。それによれば、「信託役務事業者は、故意又は過失による、本規則上の義務の不遵守により自然人又は法人に生じた損害に対して賠償責任を負わなければならない。／非適格信託役務事業者の故意又は過失による損害については、第1項で定めた損害を主張する自然人又は法人が故意又は過失を立証する責任を負う。／適格信託役務事業者については、その適格信託役務事業者がその故意又は過失なくして第1項の損害が生じたことを証明しない限り、故意又は過失はこれを推定する。／②信託役務事業者が顧客に対し事前に自身が提供する役務の使用制限について正式に告知し、それらの制限が第三者に認識できる場合は、示された制限を超える役務の使用により生じた損害については、信託役務事業者は責任を負わない。／③第1及び第2項は、賠償責任についての国内法令に従い適用される。」と定めていて、適格信託役務事業者については、自らの無過失を立証しない限り、故意又は過失が推定されることによって、立証責任の転換が図られている。¹⁸信託役務のユーザおよび署名依拠当事者は、遠隔から信託役務を利用することが普通であり、事業者側の過失と考えられる諸事情については知ることが不可能な状況にあるので、この立証責任の転換は、合理的なことである。この点は、旧電子署名指令の段階から、その第6条で、立証責任の転換を伴う損害賠償責任を認証事業者に負わせてきていたことの延長である(信託役務法6条は委託先を含めて損害賠償責任を負わせている点、前述した)。ドイツ旧署名法では、11条で故意過失に基づく損害賠償責任と、同12条で、一事故あたり最低25万ユーロの損害賠償をする補償の用意を求めてきていた。

18 Vgl. auch BT-Drucks., a.a.O. (N. 2), S. 36.

De-mail法も、同様に、一事故あたり25万ユーロの損害賠償への備えを事業者に求めており¹⁹、その点では、結果的に信頼役務法でも、そのレベルの損害賠償の備えについては求められることとなったものである（信頼役務法10条）²⁰。

損害賠償の備えを求めるのは、事業者に損害賠償の備えがなく損害賠償事故が起こった際に、当該事業者が破産して、多くのユーザおよび署名依拠当事者による役務利用が不能になってしまうといったような事態からユーザや依拠当事者を保護するために、いわば消費者保護的な要素も含んだ観点からの規制といえよう。

以上のような損害賠償責任についての法条と比較すれば、わが国では署名法上の損害賠償責任規定がなく、過失の立証が困難なユーザ側・署名依拠当事者側に損害賠償要件を立証させることになっており、これらユーザ等にとっては酷な状態が続いている点、および事業者が損害賠償によって破産等に追い込まれることを想定していない点で、再検討が必要であるといえる。

3 バリアフリー役務の提供

信頼役務について、バリアフリー化を求めているeIDAS規則15条では、「可能な限り」バリアフリーな信頼役務の提供を求めているが、同条を受けて、信頼役務法も7条でより詳細な規定をおいている。とりわけ、障害者に対するエンドユーザ製品の提供についてその情報提供をWeb上で求めているところが注目される。

わが国では、信頼役務に相当する役務についてバリアフリー化の議論はほとんどないのではないかと見られるような状況と比較すると、立法による手当として、一歩先を行く内容になっている点の一つと言ってよいであろう。

4 安全対策と法的効果に関する教示

信頼役務法の13条は、安全対策と法的効果についての教示を行うことを信頼役務事業者に求めるものである。特に同条各号すなわち、「一 提供される信頼できる役務の安全性とそれらの信頼できる使用に貢献するために必要な措置に関する情報を提供し、適切な情報機会、特に適格な信頼役務のために製品の製造業者によって提供される情報と監督機関によって提供される情報役務に注意を向ける。／二 既存の署名、電子印、またはタイムスタンプのセキュリティ価値が時間の経過によっ

19 De-mail法18条3項2号参照。

20 損害賠償への備えの具体的な細目については、損害賠償保険の付保などを信頼役務令2条が詳細に定めている。

て減少する前に、必要に応じて第15条の適格な電子署名、電子印、またはタイムスタンプ付きのデータを適切な手段で新たに保護すること。／三 提供された適格信頼役務の法的効果について周知すること。」の教示は、信頼役務を安全に利用するためには必要な情報であり、1号もさることながら、2号は、暗号技術を利用した信頼役務の技術的特性上、コンピュータの能力の向上や新たな暗号解読手法の発見等により、暗号技術の安全性の危殆化、セキュリティ価値、法的には証拠としての証明力の低下をもたらす可能性のある情報であり、例えば一旦利用された信頼役務を長期的に安全で信頼性あるものとして証拠として長期的に保存しようとしているユーザなどの場合には、知っておく必要がある情報の教示をしているものと評価できる。

わが国においては、技術的には専門家の間では当然こうした安全性の時間的低下、暗号技術の危殆化等についての知識は共有されているものと思われるが、それを信頼役務事業者経由でユーザおよび署名依拠当事者に対してまでも重要な注意事項として浸透させていく必要がある。そのための手段として事業者による教示や、次に述べる新たな保護手段・対策の提供は、不可欠なものと考えられる。

5 長期的な証拠性（検証可能性）の保持とその対策

(1) 最後に、信頼役務を利用した電子データの長期的な検証可能性の確保についての対策が問題となる。長期にわたって証拠としての性質を維持しつつ信頼役務を利用したデータを保存するためには、信頼役務法15条でさだめているように、「この点についての必要性が存する場合、適格に電子署名され、電子印が押され、またはタイムスタンプが付されたデータは、時間の経過の結果として既存の署名、電子印またはタイムスタンプのセキュリティ価値が低下する前に適切な手段によって新たに保護されなければならない。新しいセキュリティ確保は、最先端技術に従ってこれを行う必要がある。」とまで法文に書き込んで、セキュリティ確保のためのメッセージを発しておく必要がある²¹と考えられたと思われる。

電子署名やタイムスタンプが依拠している技術要素としての暗号技術は、日々進歩するコンピュータの能力や暗号解読技術の研究によって、その安全性が低下する運命にあるとされている。たとえて言えば、暗号解読技術が発見されることによって、当初は登録印レベルの安全で信頼性のある印で押印した書類が、三文判レベル

21 一般に、ユーザおよび署名依拠当事者たる第三者に対しても、この措置は必要になる。

の誰でも打てるような印の安全性レベルに低下すると考えてもらえばよいであろう。そうしたリスクに対しては、安全性が低下する前に、より安全な暗号技術（安全なアルゴリズムand/or安全なパラメータ）を使った電子署名で元の署名済みデータをカプセリングすることが対策の一つとして考えられている。

技術的に実用化されている電子署名技術を用いた一般的な手法としては、電子署名で用いられる長期署名フォーマットを利用して署名済みデータのファイルに安全なタイムスタンプ（これも安全な暗号技術を用いている。）を利用して、安全性が低下する前に（より）安全なタイムスタンプを重ね打ちしていく方法が標準化されているが、²²そうした手法を技術中立的に信頼役務法15条は定めているといえる。データの安全性については、こうしたアプローチが対策の一つとして技術中立的に法定されているのである。

（2） また、一方で、データの長期的な検証可能性だけではなく、本人確認資料や証明書の失効データなどの信頼役務事業者が有するデータや書類等についても、長期的に保存しておく必要性もありうる。実際の署名利用のプロセスにおいては、本人確認がどの資料に基づいて確実になされたのか否かや（証明書発行段階でのなりすましの有無の確認）、証明書の失効を事故があった直後にただちになしたのかどうか²³などが検証されることになる。この点については、eIDAS規則では、長期的な検証可能性を確保するために、適格信頼役務事業者に対して、その24条2項（i）において、業務終了時の計画を立案させるように規定している。業務の休廃止や破産等により業務の継続が困難になるときに、他の事業者への引き継ぎ等の努力をさせるように差し向けるために計画の立案を求めているわけである。しかし、計画だけでは、業務の引き継ぎが現実になされるかどうか問題が残ると言わなければならない。

22 拙稿・前掲注1）41頁注27参照。これは、新しい安全なタイムスタンプが打たれた日時においては、未だもとのタイムスタンプの安全性が低下しておらず（有効であり）、データの完全性等および打刻日時等（タイムスタンプの証明事項）に問題がないということを証明することによる。このロジックを複数回繰り返しても、条件を満たす限り電子署名と署名時タイムスタンプまたは検証後のアーカイブタイムスタンプ（アーカイブ用タイムスタンプ）の打刻日時には問題がないことが証明されることになる。

23 認証事業者による失効が遅れると、例えば盗難・漏洩・紛失した秘密鍵が第三者により悪用されてしまいそれを用いた署名が署名の検証上有効なものとされてしまう事態になる可能性があり、そうした事態を防止するためには、証明書の失効時点がいつであったか、ただちに失効手続がとられたのかといった点についての失効記録情報が検証される必要が訴訟等の中に出てくることになる。

それに対し信頼役務法では、その15条で、引き継ぎ事業者が確保できないときの最終的代替策として、同条1項1段2号は、「二 第5項で言及されている信頼インフラストラクチャにおいて連邦ネットワーク庁によって引き継がれる」可能性を国家として確保している点が注目される。この点も、従来の旧署名法以来の制度的な対応の再現であり、長期的に検証すべきデータの検証条件を国家による、書類²⁴・データ（公開鍵データベース、失効情報データ）等の引き継ぎ保存により保障する制度として、注目されるものである。旧署名法時代から、現実にすでに業務を休廃止した事業者の書類等を連邦ネットワーク庁が引き継いで、書類等の消失を防いでいる状況であることは、電子証拠の長期的な検証可能性の確保という観点からは極めて注目に値する制度であるといえよう。なお、オーストリア法においても、同様の仕組みをとって長期的な検証可能性の確保の措置を執ることとしていることについては、前述²⁵したが、同様に注目される制度になっている。

V おわりに

別稿で検討してきたeIDAS規則を実施するものとしてドイツで制定された信頼役務法は、上記のような内容と特徴を持っているものである。前章では、信頼役務法のプラス面が出過ぎたような検討結果となってしまったが、しかし、同法の特徴とわが国の電子署名法の課題を照射するものとしての意義は、極めて大きいものがあるといえる。eIDAS規則と合わせた信頼役務法の見るべき点をいくつか紹介検討したことから本稿を閉じることにしたい。

〔後注〕本稿は、JSPS科学研究費補助金（課題番号16K03291）の補助を受けた研究成果の一部である。記して感謝の意を表したい。

24 適格証明書の継続的な検証可能性への配慮と題する信頼役務令（VdV）4条は、証明書と失効情報のデータおよび書類の他業者または連邦ネットワーク庁への引き継ぎについて定めているが（同条1項）、書類については、可能で合目的である限りで、電子化して引き継ぐことを義務づけている（同条2項）。

25 前述・前掲注12参照。